UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/643,678	08/18/2003	Sundeep M. Bajikar	42P16632	4611

45209 7590 11/09/2009

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
11/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/643,678	BAJIKAR ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 9-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 9-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on July 17, 2009 has been entered. Claims 1-7, 9-34 are pending. Claims 1, 7, 10, 11, 26, 28, 29, 30, 32 amended and Claims 33, 34 are newly added by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 2, 7, 9-11, 23, 24, 26-28, 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krancher et al (US Patent No. 6,799,237) in view of Seeker et al (US Patent No. 6,141,757) and in view of Lee (US Patent No. 7,275,109).

As per claim 1, Krancher teaches a docking connector, and the docking circuit coupled to the bus and coupled between the bus and the docking connector which provide filtering mechanism to prevent the data from being provided to a device external to the computer system through the docking connector [Fig.1, 3, associated text]. Krancher does not expressively mention a secured docking circuit to scan for the trusted data cycle.

However, Seeker teaches: a chipset; an internal component of the computer system [Fig. 1]; a bus coupled to the chipset to communicate a trusted data cycle to the internal component of the computer system [Fig. 1, col. 2 lines 35-39]; a connector; and a secure docking circuit coupled to the bus and coupled between the bus and the connector [Fig. 1, component 200] to scan for the trusted data cycle, detect the trusted data cycle [Fig. 1, col. 2 lines 40-54], and provide a filtering mechanism to prevent the trusted data cycle from being provided to a device external to the computer system through the connector [Fig. 1, col. 2 lines 40-54, col. 3 lines 51-60, col. 9 lines 19-26].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Seeker with Krancher, since one would have been motivated to provide security protection for communications via a bus for a computer [Seeker, col. 1 lines 20-22, 44-46].

Seeker teaches scanning the trusted data cycle, wherein the trusted data cycle includes the identification information. Krancher and Seeker do not expressively mention detect trusted data cycle by detecting a predefined trusted data cycle indicator value.

However, Lee teaches: detect trusted data cycle by detecting a predefined trusted data cycle indicator value [Figs. 3, 4, authenticated-command bit 31, information/command 34, 42, 44].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Lee with Krancher and Seeker to data set with identifiable portion, since one would have been motivated to authenticate the

communication between the entities and prevent the attack [Lee, col. 1 lines 7-8, col. 2 lines 35-51].

As per claim 2, the rejection of claim 1 is incorporated and Krancher discloses: wherein the bus is a Low Pin Count bus [col. 4 lines 39-40].

As per claim 7, Krancher teaches: a Low Pin Count bus [col. 4 lines 39-40], a docking connector, and the filtering means is coupled between the bus and the docking connector which scans the trusted data cycle on the bus and prevents the trusted data cycle on the bus from being accessed by an unauthorized component coupled to a connector, wherein the filtering means is coupled between the bus and the connector [Fig.1, 3, associated text]. Krancher does not expressively mention filtering means for scanning for trusted data cycles.

Seeker teaches:

filtering means for scanning for trusted data cycle on the bus and preventing the trusted data cycle on the bus from being accessed by an unauthorized component coupled to a connector, wherein the filtering means is coupled between the bus and the connector [Fig. 1, col. 2 lines 35-54, col. 3 lines 51-60, col. 9 lines 19-26].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Seeker with Krancher, since one would have been motivated to provide security protection for communications via a bus for a computer [Seeker, col. 1 lines 20-22, 44-46].

Seeker teaches scanning the trusted data cycle, wherein the trusted data cycle includes the identification information. Krancher and Seeker do not expressively mention each include a predefined trusted data cycle indicator value.

However, Lee teaches: trusted data cycles that each includes a predefined trusted data cycle indicator value [Figs. 3, 4, authenticated-command bit 31, information/command 34, 42, 44].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Lee with Krancher and Seeker to data set with identifiable portion, since one would have been motivated to authenticate the communication between the entities and prevent the attack [Lee, col. 1 lines 7-8, col. 2 lines 35-51].

As per claim 9, the rejection of claim 7 is incorporated and Krancher discloses: means for monitoring data cycle on the LPC bus [Fig.1, 3, associated text].

As per claim 10, Krancher teaches a docking connector, and the docking circuit coupled to the bus and coupled between the bus and the docking connector which provide filtering mechanism to prevent the data from being provided to a device external to the computer system through the docking connector [Fig.1, 3].

Seeker teaches:

monitoring for communication of trusted data cycles on a bus with a secured docking logic of a computer system [Fig. 1, col. 2 lines 35-54, col. 3 lines 51-60, col. 9 lines 19-

26]; detecting each of the trusted data cycles by detecting a predefined trusted cycle indicator with the secured docking logic [col. 3 lines 55-60]; preventing the trusted data cycles from being available to a component external to the computer system with the secured docking logic [Fig. 1, col. 2 lines 35-54, col. 3 lines 51-60, col. 9 lines 19-26].

Seeker teaches scanning the trusted data cycle, wherein the trusted data cycle includes the identification information. Krancher and Seeker do not expressively mention a same predefined trusted data cycle indicator at a beginning of each of the trusted data cycles.

However, Lee teaches: a same predefined trusted data cycle indicator at a beginning of each of the trusted data cycles [Figs. 3, 4, authenticated-command bit 31, information/command 34, 42, 44, col. 6 lines 8-9, 25-31].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Lee with Krancher and Seeker to data set with identifiable portion, since one would have been motivated to authenticate the communication between the entities and prevent the attack [Lee, col. 1 lines 7-8, col. 2 lines 35-51].

As per claim 11, the rejection of claim 7 is incorporated and Lee discloses:

wherein the trusted data cycles begin with the predefined trusted data cycle indicator of "0101" [Figs. 3, 4, authenticated-command bit 31, information/command 34, 42, 44, col. 6 lines 8-9, 25-31].

As per claims 23 and 24, the rejection of claim 1 is incorporated and Seeker discloses:

wherein the circuit makes a data cycle that is not a trusted data cycle available to the device external to the computer system [col. 9 lines 20-26].

As per claim 26, the rejection of claim 1 is incorporated and Lee discloses:
wherein the trusted data cycle begins with the predefined trusted data cycle indicator [Figs. 3, 4, authenticated-command bit 31, information/command 34, 42, 44].

As per claim 27, the rejection of claim 10 is incorporated and it encompasses limitations that are similar to limitations of claim 23. Thus, it is rejected with the same rationale applied against claim 23 above.

As per claim 28, the rejection of claim 1 is incorporated and Seeker discloses:
the trusted data cycle comprises plaintext format data [col. 3 liens 58-59].

As per claim 33, the rejection of claim 1 is incorporated and Lee discloses:
each trusted data cycle hash the same predefined trusted data cycle indicator value [Figs. 3, 4, authenticated-command bit 31, information/command 34, 42, 44].

3. Claims 3-6, 12-19, 29-32, 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krancher et al (US Patent No. 6,799,237) in view of Seeker et al (US Patent No. 6,141,757) and in view of Lee (US Patent No. 7,275,109) and in view of Strongin et al (US Patent No. 6,832,317).

As per claim 3, the rejection of claim 1 is incorporated and Strongin discloses: wherein the component provides protected memory storage [Fig. 4, 7A, 7C, 7D].
Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Strongin with Krancher, Seeker and Lee, since one would have been motivated to provide security to the personal computer components [Strongin, col. 2 lines 21-29].

As per claim 4, the rejection of claim 1 is incorporated and Strongin discloses: wherein the component provides platform authentication [Fig. 4, 7A].

As per claim 5, the rejection of claim 1 is incorporated and Strongin discloses: wherein the component maintains a protected path between the chipset and a keyboard [Fig. 4, 29A].

As per claim 6, the rejection of claim 1 is incorporated and Strongin discloses: wherein the computer system is a notebook computer [Fig. 39B].

As per claim 12, the rejection of claim 10 is incorporated and Strongin discloses: communicating trusted data cycles between the chipset of the computer system and a first component of the computer system that provides cryptographic capabilities [Fig. 4].

As per claims 13 and 15, the rejection of claims 12 and 14 are incorporated and Seeker discloses:

the communication of the trusted data cycle between the chipset and the first/the second component is in plaintext format [Fig. 1].

As per claim 14, the rejection of claim 10 is incorporated and Strongin discloses:

communicating trusted data cycles between a chipset of the computer system and a second component that provides trusted input capabilities [Fig. 4].

As per claims 16 and 17, the rejection of claim 15 is incorporated and Strongin discloses:

the second component maintains a protected path between the chipset and a keyboard, wherein keystroke data is communicated by the chipset to protected memory and trusted applications [Fig. 4, 7A, 7C, 7D].

As per claim 18, the rejection of claim 12 is incorporated and Strongin discloses:

wherein the first component protects secret data of the computer system by encrypting the secret data [Fig. 4, 7A, 7D].

As per claim 19, the rejection of claim 12 is incorporated and Strongin discloses:

wherein the secret data is decrypted by hardware of the computer system [Fig. 29A, associated text].

As per claim 29, Krancher teaches a docking connector, and the secured docking circuit coupled between the bus and the docking connector which provide filtering mechanism to block the trusted data cycle from an external device coupled with the docking connector [Fig.1, 3, associated text].

Seeker discloses:

a chipset, a first internal component; a second internal component; a bus coupled to the chipset, coupled to the first internal component, and coupled to the second internal component [Fig. 1], the bus to communicate a trusted cycle data from the chipset to the first internal component [Fig. 1]; a connector and secure docking logic couple between the bus the connector, the secure docking logic to block the trusted data cycle from an external device coupled with the connector [Fig. 1, col. 2 lines 40-54, col. 3 lines 51-60, col. 9 lines 19-26].

Seeker teaches scanning the trusted data cycle, wherein the trusted data cycle includes the identification information. Krancher and Seeker do not expressively mention the trusted data cycle having a predefined trusted data cycle indicator.

However, Lee teaches: the trusted data cycle having a predefined trusted data cycle indicator [Figs. 3, 4, authenticated-command bit 31, information/command 34, 42, 44].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Lee with Krancher and Seeker to data set with identifiable portion, since one would have been motivated to authenticate the

communication between the entities and prevent the attack [Lee, col. 1 lines 7-8, col. 2 lines 35-51].

Strongin teaches:

a chipset; a first internal component to provide at least one hardware cryptographic functionality selected from hardware protected storage, platform binding, and platform authentication [Fig. 4, 7A, 7D]; a second internal component to provide a trusted input capability from a keyboard [Fig. 29A].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Strongin with Krancher, Seeker and Lee, since one would have been motivated to provide security to the personal computer components [Strongin, col. 2 lines 21-29].

As per claim 30, the rejection of claim 29 is incorporated and Seeker discloses:
the trusted data cycle comprises plaintext format data [col. 3 liens 58-59].

As per claim 31, the rejection of claim 30 is incorporated and Lee discloses:
the predefined trusted data cycle indicator comprises 0101 [col. 6 lines 25-31].

As per claim 32, the rejection of claim 29 is incorporated and Seeker discloses:
the secured docking logic comprises a circuit [Fig.1].

As per claim 34, the rejection of claim 29 is incorporated and Krancher teaches: the bus comprises a Low Pin Count bus [col. 4 lines 39-40].

4. Claims 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krancher et al (US Patent No. 6,799,237) in view of Seeker et al (US Patent No. 6,141,757) in view of Lee (US Patent No. 7,275,109) in view of Strongin et al (US Patent No. 6,832,317) and in view of Probst (US Patent No. 5,982,899).

As per claim 20, the rejection of claim 18 is incorporated and Probst discloses:
the first component merges data with configuration values of the computer system [Fig. 1, col. 5 lines 18-39].
Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Probst with Krancher, Seeker, Lee and Strongin, since one would have been motivated to verify configuration of a computer system and prevent altering or bypassing the computer system information [Probst, col. 4 lines 62-63].

As per claim 21, the rejection of claim 18 is incorporated and Probst discloses:
wherein the first component requests a system identification request [col. 7 lines 13-17, 34-35].

As per claim 22, the rejection of claim 21 is incorporated and Probst discloses:

wherein a trusted third party chip verifies an identification of the computer system and sends a response to the first component [col. 3 lines 49-59, col. 7 lines 36-63].

5. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krancher et al (US Patent No. 6,799,237) in view of Seeker et al (US Patent No. 6,141,757) in view of Lee (US Patent No. 7,275,109) and in view of Yanagisawa (US Patent No. 6,519,669).

As per claim 25, the rejection of claim 1 is incorporated and Yanagisawa teaches the circuit blocks the data cycle from a docking connector [Fig. 1, 2].
Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Yanagisawa with Krancher, Seeker and Lee, since one would have been motivated to control docking and undocking a peripheral device while a computer system is in operation [Yanagisawa, col. 1 lines 9-11].

Response to Amendment

6. Applicant has amended claims 1, 7, 10, 29 to include the limitation "detect the trust data cycle by detecting *a predefined trusted data cycle indicator value*", or "trusted data cycles that *each include a predefined trusted data cycle indicator value*" or detecting a *same predefined trusted data cycle indictor at a beginning of each of the trusted data cycles*", which necessitated new ground of rejection. See new ground of rejection based on previously cited prior art and in combination with the newly found

reference Lee (US 7275109). Therefore, the applicant's arguments, filed on July 17, 2009, are moot in view of the new ground(s) of rejection. Lee discloses authentication transmission, which includes authenticated-command bit 31, information/command 34, and fields 42, 44 as shown in Figs. 3, 4. The fields 31, 34, 42, 44 include predefined indicator value at a beginning of each of the authentication transmission [Figs. 3, 4, authenticated-command bit 31, information/command 34, 42, 44, col. 6 lines 8-9, 25-31]. Therefore, Lee teaches the amended claim limitation. In this case combination of Krancher, Seeker and Lee is sufficient because one of ordinary skill in the art at the time the invention was made would be motivated to combine Seeker with Krancher to provide security protection for communications via a bus for a computer by scanning for the trusted data cycle and further to combine Lee with Krancher and Seeker to authenticate the communication between the entities and prevent the attack by utilizing the authentication transmission between the entities.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/N. P./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435